Information Technologies for the Information Agent

Sérgio Tenreiro de Magalhães[1], Henrique Santos[1], Leonel Duarte Santos[1], Kenneth Revett[2] and Paulo Viegas Nunes[3]
[1]University of Minho, Guimarães, Portugal
[2]University of Westminster, London, UK
[3]Military Academy Research Center (CINAMIL), Lisboa, Portugal
psmagalhaes@dsi.uminho.pt
leonel@dsi.uminho.pt
revettk@westminster.ac.uk
pfv@net.sapo.pt

Abstract: The information agent has requirements in the Information Technology (IT) age that are in everything comparable to those of one hundred years ago. But, despite being similar, they require new forms of implementation due to the evolution of the communication platforms and protocols and to the increase in the amount of information that has to be known, stored, transmitted, and interpreted. Although, in many situations, the information agent will make use of everyday equipment, he will always require levels of trust in the processes that are far beyond those of the everyday citizen. But this cannot imply to carry huge infrastructures that will reveal the agent's intentions. In extreme situations the information agent is the soldier engaged in military activities in hostile environments. There, above all places, he requires light weight trustable equipment and protocols that can perform those tasks.

This work, while making the parallel with the traditional methods, proposes a technological environment able to give answer to the requirements of information agents dealing with the need for a competitive intelligence advantage through the correct use of IT, namely biometrics, alternative authentication processes, Public Key Infrastructures and anti-fishing technologies.

Keywords: Security infrastructure, wearable security, information activities

1. Introduction

The information age has arrived and, with it, the need to manipulate the huge amount of data that is collected and the world of advantages that arise from the knowledge that is created from it. In the last few years the capability to collect, process and transfer information has increased in a way that allows functionalities never before imagined. But this gigantic infrastructure is frequently shared by many different users with different needs for security. Classified information travels, at the best protected by Virtual Private Networks (VPNs), in the same physical support used to transmit personal and professional e-mails, publicity, academic information or online game's data. Sometimes the communication between devices is so natural that we don't even think about it (Figureure 1). For instance, the communication between a mobile phone and a bluetooth headset is now so natural that we don't even think on the fact that the information is travelling between one device and the other.

On the other hand, thanks to this easiness of communication, data can be transferred not only from one device to another, but also from the devices to a central unit with a higher processing capability. Therefore, an information agent can receive at any moment an update on his knowledge that might be relevant for the next process of decision making. This can be done by many means, Short Message Service (SMS), by a telephone call, an e-mail (accessed on a laptop, a palmtop or a mobile phone), or by augmented reality. In this last case, the data is included in the sensorial stimulation of the environment, for instance by including extra information on a windshield of a car or in the inner lens of sunglasses (Figureure 2). This can be very helpful when it is necessary to confirm one certain alleged identity, using biometric authentication algorithms (voice, face, etc.), or if instructions on a sequence of actions are required, for instance the sequence of steps necessary to urgently repair a given instrument, using the same technology that applies virtual reality concepts to e-learning (Liarokapis et al., 2002).

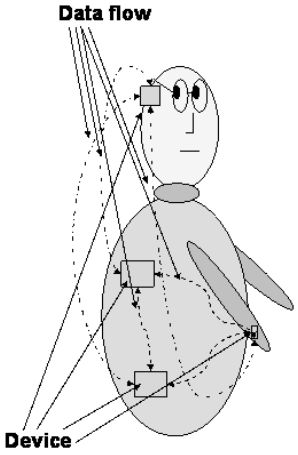

Figure 1: Several wearable devices can autonomously communicate between them, both in wired and wireless ways, both encrypted and unprotected.

Figure 2: Relevant information can be added into the image seen through an object. In this case the windshield of a car includes the information that one certain vehicle is referenced in one certain database, after an automatic identification of the licence plate.

If an information is likely to be required it can be previously downloaded into a storing device, for instance if an agent is about to meet someone and requires an identity confirmation he can download that person's biometric pattern and obtain an identity confirmation once they are together. If the identity confirmation is not programmed, the information can be transferred to a central server that will process the data and return the desired information. But all these functionalities bring us back to the traditional issues: confidentiality, integrity and availability of the information. The issue of availability is not on the agent's side of this technological infrastructure and, therefore, is out of scope for this work. We'll now focus on how Public Key Infrastructures (PKI) and biometric technologies can be of assistance in solving the confidentiality and integrity issues.

2. The public key infrastructure (PKI)

Most of the threats directly related with the communication infrastructures can be mitigated by cryptography. From all the tools and techniques available, those based on public key algorithms are especially interesting since they avoid the exchange of secret keys in an open environment, like the Internet (Schneier, 1996, Kaufman et al., 2002). This way we transfer the security problem from the message itself to a key pair (public key and private key), which is a simpler entity to take care of.

In fact, to securely communicate with someone, besides the required tools (a lot of them in public domain), all we need is to give our public key to everyone/everything that wants to communicate with us, and get the public key of those we want to communicate with. Information encrypted by one of the keys can only be decrypted by the other. Processing the message with a hash function and encrypting the result is a perfect way to implement an electronic signature. This is easy to deploy within small groups of users/devices which know each others. However, if we try to scale the solution to larger groups of distant and unknown users, the (old) trust issue about the presumed owner of a certain public key arises.

To solve this problem we can use a certificate, which is a data structure containing the public key, cryptographically signed by a trustable third party, a Certificate Authority (CA). It is assumed that we have the CA's public key and we trust this entity to what concerns its ability to certificate every pair user/public-key. Again, we are trying to transfer the security problem from a larger uncontrolled domain to just one key, but this time assuming its owner has a tremendous power to handle a huge number of public keys. Due to economical and geographic distribution issues, a CA typically relies on local Registration Authorities (RA) to verify user authentication during the certification requesting phase. Finally, a CA must keep actualized information about good and compromised or non-valid keys and provide a way to store and give access to public keys (key management). This kind of structure is called a PKI (Public Key Infrastructure).

PKIs have been around for several years, but there are few examples of well succeeded deployments, especially in large scale organizations where people do not know each other. Application integration is another obstacle. Most of the solutions available require external applications and some specific training to use them. Today e-mail clients are an exception and it is now possible to find many that supports a cryptographic public key algorithm. With these recent achievements it is not a surprise to find some recommendations about how to deploy large scale PKIs, particularly in the public sector (Gritzalis, 2005). However, there are some issues we need to take care of. For instances, the PKI security depends on the CA's Security Police, which could be incompatible with the Security Police of each organization/department that is using it. But even worst, at a public sector scale, the users' know-how is very different and there is always the possibility to compromise a private key or to fraudulently use a public key. To mitigate this lasts vulnerabilities a strong authentication is necessary and biometric technologies provide that extra level of security not only in the case of human-device interaction, but also in the case of device-device interaction if a human is wearing the device (technological enhanced glasses, watches, etc.).

3. Wearable technologies

Technological clothing is starting to reach the market, although it is still focused on the entertainment technologies. But a wither technological infrastructure can be fully integrated with clothing, using multilayered fabrics (Figureure 3 and 4) that create a dry level for implanting hardware, a comfortable layer that is close to the body and an energy supplying layer that will allow the transportation of power supply to the devices (Magalhães et al., 2005) This technology can be used for everyday use or for some specific needs. In the case of the information agent, this kind of apparel can permanently monitor the biometric data of the information agent (heart beat rate, breathing rate, etc.) in order to inform the central unit in case of abnormal situations and to insure that the apparel is still in use by the same person that provided some kind of authentication some time ago (when starting the system, probably after dressing). This can be the mechanism that

enables the use of PKI between devices without the danger of establishing a communication not desired by the information agent at a given moment.

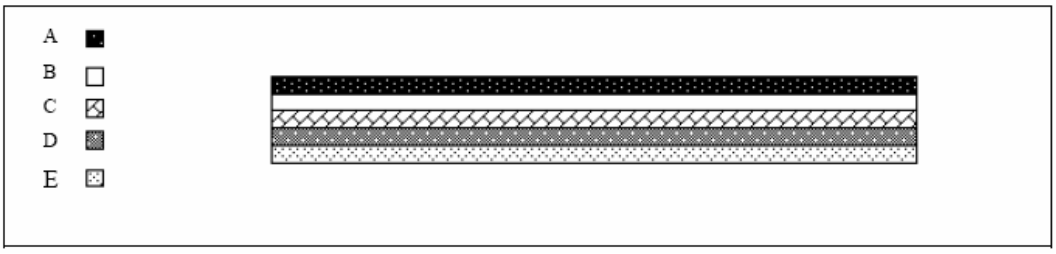

Figure 3: Schematic diagram of the cross section of a multi-functionalized structure of a fabric with an all-over effect or layered structure.

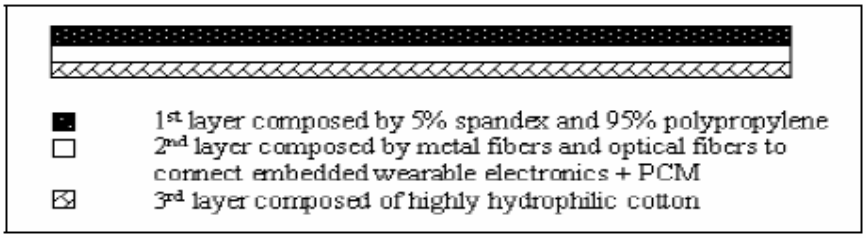

Figure 4: Example of cross-section of a concrete fabric structure.

4. Biometric technologies

Biometric technologies are mainly used in both physical and logical access control (Luis-García et al., 2003) but they can also be used to assist in other tasks, some so unimaginable has helping to preserve several animal endangered species (Jewell et al., 2001) From the information agent activity, the most useful classification of the biometric technologies is the division between Stealth (technologies that can be used without the knowledge of the user) and Cooperative technologies (technologies that demand the collaboration of the user), although the most used criteria is related to the characteristics used in the process, dividing these technologies in behavioural and physical..

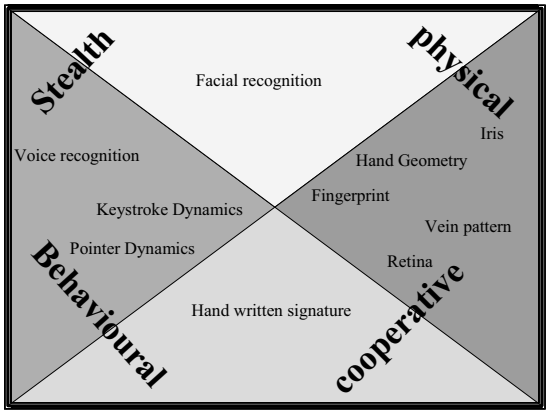

Figure 5: Shows the classification of the most commonly used technologies according to both criteria

All the stealth biometric technologies can assist the information agent in authenticating/identifying individuals. Some can even assist in the detection of repeated patterns than can indicate that the agent is being followed. In this matter the existing knowledge on computer vision can also assist on the identification of other relevant factors in the landscape, like known vehicles.

But, as mentioned before, the information agent also requires strong authentication processes that can create an extra layer of security into the confidence chain of the PKIs and that can grant them, and only them, access to remote servers where they can download and upload sensitive information. That can be achieved with any biometric technology (ones with more accuracy then others) but it is desirable that it can be used without revealing the intentions/activities of the agent. Therefore, the use of specific devices, used to capture particular characteristics like fingerprints, should be avoided. Being so, the most adequate biometric technologies are those that can find a pattern from normal behavioural like, for instance, the way an agent types a password or a personal identification number (PIN) on a portable device. This last technology is known as keystroke dynamics. But passwords have known issues, like the tendency to use only two or three passwords for all the used services. In fact passwords have a contradiction in themselves once they must be complex in order to provide a certain level of security and they must be frequently changed. But, on the other hand, they must be easy to memorize, therefore simple (Wiedenbeck et al., 2005). We believe that the solution, when using small portable devices that can be protected from eyesdropping, is to substitute the alphanumeric secret sequence, by a secret made of a sequence of clicks in an image, the graphical authentication.

4.1 Graphical authentication

Graphical Authentication is a technology in which the user selects some images from a bigger set, or selects some points in an image. The secret possessed by the legitimate user is the images/points selected and the corresponding sequence, called a passgraph. These technologies can provide a way to generate traditional passwords from the sequence of images/points selected and, in this way, provide compatibility with the existing systems. In this section we will show how passgraphs can be converted to strings using unidirectional functions and how Graphical Authentication Systems (GAS), while being used for authentication, can also be used to prevent impersonation of websites, allowing not only the user's authentication but also the system's authentication towards the user.

5. Authenticating the user and the service

In our proposed system, when the user creates a username in the system he also uploads an image that will be used for the insertion of the passgraph, the secret sequence of clicks that will grant access to the web application. At the upload moment, the user must be briefed of the best practices on choosing images and sequences of points in order to maximize the quality of the security provided, for instance he should not choose images with faces and them select the eyes, nose, mouth or any other points that are most appealing (Magalhães et al., 2006). The user must also understand that the use of passgraphs increases the quality of the secret used (by expanding the key space) without increasing the effort on memorizing or introducing the secret, but he must also be aware that this presents no advantage if he does not protect the privacy of his passgraph, that is hard to voluntarily transmit to others but is vulnerable to eyesdropping.

When a registered user intends to access the service, he inserts his username and the system creates the corresponding login page that includes the image that is specific to that user (Figureure 6). If the system does not present the correct image, the user knows that he is most probably dealing with an impersonation of the server and does not proceed with providing the authentication data.

For these systems to coexist with the traditional authentication processes, it is desirable to possess a converter that can generate strong passwords from the sequence of clicks, but that doesn't create new vulnerabilities. The next section presents our conversion system.

Figure 5: Graphical authentication procedure with server authentication. The user first introduces his username and then the system presents the associated image for him to insert his passgraph

5.1 Generating a password from a passgraph

A passgraph with length n will be a vector of the type (p1, p2,…, pn) where $p \in \{(x,y) \mid 0 \le x \le 19,\ 0 \le y \le 13\}$. The values of x and y define the selected section in a specific two-dimensional image. In order to maintain the compatibility with the traditional password systems, we need to generate a string. For that, we'll use 15 tables, numbered from 0 to 14, with 26 columns and 20 lines. So we have 7800 cells, each one with one 3 characters string and the corresponding ANSI code. Figureure 7 is one of those tables.

													0												
4kQ	v9;	D't	~\'	M'p	K"|	.n.	@8v	(!p	LQi	H=p	j,6	h$m	,:]	q;	]h8	D-{	-Yh	`Rj	T^-	evf	y6:	i*f	jJH	^sl	{{T
E6W	xnf	:}V	Sx8	e(r	XT0	;8u	aWA	x6w	pd/	#,T	t4j	EwB	;!^	ElX	VOU	PjE	br4	wch	;!I	A:/	*eb	D,S	8R1	8%j	dQi
B`o	}5N	yDv	y$U	;3t	F`|	[+-	X!g	yvd	HdF	9XQ	Wcp	2-u	pEB	}Tj	jZI	_mx	f#l	5Df	&)^	?d$	up6	3:@	u=	r<	ylK
T~3	LZM	hF7	.'V	]`d	C}{	-5%	];3	qwn	&!n	-vf	sTr	lrV	X3d	aZn	zs4	HqV	l1U	@v>	AUs	L[a	?/n	OkA	|S/	=s/	j<6
ZU8	xtx	yT2	ekN	Evy	V^#	)l2	2Fv	<w&	u{=	l6L	?f0	\r.	Jew	6l/	zL]	`Oc	zJk	Ati	Y&h	xG\	O]^	L3E	P#D	8.d	tfx
!Z[	He$	'Ot	HdS	QB(	>,y	ewC	}{d	ayq	%+"	a")	0LY	_DE	NjD	53l	xXV	ry6	~,Y	;l6	({e	$,8	D~2	,Mp	IL9	-zl	Ad~
aC&	@,H	jos	Hg4	e$Q	(i?	0f|	k;n	hpS	Dx$	z0&	?P3	W#f	k:B	&k`	v#^	O/t	0)q	48a	4~!	sv\	N.!	gZb	~"J	?{<	zaL
~t	0lp	:%S	%$K	bUb	`f-	`9(	3'"	u<W	HKl	@m=	CTQ	O)H	no;	A-t	{!#	Q\)	rGc	1TX	|Vy	`<o	l7B	~Np	" "	3^$	gYr
P?p	x7U	&^"	FLn	F|.	,\b	1jo	4{E	L$4	_##	6Bv	h8]	e@J	KFP	cO&	}SN	$kS	fN!	b(!	-%w	i]/	c7`	#P:	;an	2=!	q^4
k2"	v0n	z$S	v4j	W?,	,yL	$#u	-q)	&O}	wZt	\G]	}5B	k\a	BK6	Xhp	m=c	[(Q	Tkd	+!r	!Y^	IMf	KVf	jjM	rjJ	tF#	+v(
-md	eYY	t4Y	ali	v!l	cT6	Ml@	wsk	8Bo	jES	|9R	#&.	N.k	;??	(*V	h*i	0@^	^1"	xB$	-lv	<.t	Kb/	V9<	&2m	:,0	D#r
ZVW	j.W	X~O	/f3	g@5	p%h	rAM	kuv	B[9	xzb	UQR	4"b	gIN	S6*	@6}	j)6	UMr	z*H	n.K	O-H	8el	<>r	4H2	t[/	p;P	ZVw
WKA	.y>	?"B	XDw	+q,	OQ"	DNL	]d1	9lf	A[7	/Y'	j8\	h|1	CF*	DV:	tot	(>~	}4H	y%3	V[o	*s	!5Q	ey&	$o\	d(%	o(@
]04	e5Y	$rB	&q@	~~E	?<!	3[/	ZG	"MD	9t[	{DF	|zU	D`d	6B~	Z?|	tjI	8o+	RFi	~W3	s7F	?Sj	]V[	`RS	.5q	xke	dgQ
"M:	OCn	G%k	wyv	R~o	9kb	7uM	gCa	.|.	2G1	'Ew	CFi	Ljz	v+d	#1&	/e$	oxG	-o2	U`j	3k!	<2q	#wE	<ub	Z2T	Ig$	zK'
ggz	t4%	\a:	J\2	{[	ky>	|kI	K07	&6x	:N:	>5V	}eg	>L2	2su	Cb^	M)(	3?T	Z|*	-^D	gUr	>LI	=C:	rMS	b^~	>6/	pte
W&H	!bQ	:Ww	dbX	P6U	AkE	`7K	G#%	u6V	TN9	A:3	1Q(	:L5	Gm-	@HA	'jc	Zs[	>N/	c;?	n,>	0rW	5}}	qQ(	B3l	*Bh	#Ti
!~z	UxU	veV	H~?	;b#	S80	:=?	HXd	^H~	y!1	Tt*	.db	V}7	Ff!	XYt	P=W	iKO	t-3	w1|	ubN	Wsk	\Ko	W8x	vbu	+q2	]),
Ud.	@yL	cc[	tba	1wP	sXB	LGk	-'A	sSC	dxU	~6Z	A6r	7[m	1v%	R'M	"7]	~`k	W&5	lXl	62]	tDn	V#R	LLj	pHp	XHm	v=G
}C!	a:E	<qM	QG#	w(@	M&,	[<@	!QP	yn*	*D~	s2W	y4@	VJ'	do*	TU"	,<B	SRA	x9t	K,I	DzC	_6-	S,8	~Q]	).?	N^}	hVY

Figureure 6: The conversion of the passgraph to traditional passwords (creating strong passwords) is made through unidirectional functions that make use of 15 tables similar to this one.

We find our first cell by locating, in the number (x+y)mod15 table, the line x and column y. Then, for each $p \in \{(x,y) \mid 0 \le x \le 19,\ 0 \le y \le 13\}$ we'll do:

- $\left(x + y + 1^{st}\ ANSIFromThe\,\mathrm{Pr}\,eviousSelectedCell\right) \bmod NumberOfLines$ to find the next line selected;
- $\left(x + y + 2^{st}\ ANSIFromTh\,e\,\mathrm{Pr}\,eviousSelectedCell\right) \bmod NumberOfCo\,lums$ to find the next column selected;
- $\left(x + y + 3^{st}\ ANSIFromTh\,e\,\mathrm{Pr}\,eviousSelectedCell\right) \bmod NumberOfTa\,bles$ to find the next table selected;

To prevent the possibility of discovering the sequence of clicks from the string if this is compromised, for instance by capturing the packages on a poorly encrypted network, we need to make some final changes in the string. In this way, frequent changes in the tables (and the correspondent passwords) can increase the level of security of the system, in a transparent way to the user that will continue to click in the same places of the same Figures. In our case:

> Let x be the ANSI code of the first element of the so far generated string. Given t = x mod n, will reverse the order of the first t characters.
> Let y be the ANSI code of the last element of the so far generated string. Given k = x mod n, will reverse the order of the last k characters.

5.1.1 Pointer dynamics

Pointer Dynamics is still an experimental concept in which a biometric algorithm aims to define a user's clicking pattern when using a pointing device (mouse, stylus, touch pad, etc.) to authenticate towards a Graphical Authentication System. In each login attempt, access is granted if and only if the pattern exiting in the way the secret was clicked matches the user's known and recorded pattern. This is a concept already in use for passwords, called keystroke dynamics, but recently adapted to graphical authentication. Given its youth it is quite normal that the accuracy levels are still not satisfactory but research is on the move to change that.

6. Conclusions

The information technologies are creating a world of new opportunities for the information agent, supplying on real-time critical information, allowing bidirectional communication to central repositories, and allowing autonomous communication between devices. But all these opportunities raise the challenge of assuring confidentiality and integrity of the data, therefore we need to find new protocols, not only technological but also behavioural, to ensure its correct use. This paper shows that wearable technologies combined with graphical authentication procedures can be of assistance on this task.

References

Gritzalis, S. (2005) A good-practice guidance on the use of PKI services in the public sector of the European Union member states. *Information Management & Computer Security,* 13, 379-398.

Jewell, Z. C., S.K., A. & Law, P. R. (2001) Censusing and monitoring black rhino (Diceros bicornis) using an objective spoor (footprint) identification technique. *J. Zool*, 1-16.

Kaufman, C., Perlman, R. & Speciner, M. (2002) Private Communication in a Public World. *Network Security.* Second Edition ed. Upper Saddle River, NJ 0745, Prentice Hall PTR.

Liarokapis, F., Petridis, P., Lister, P. F. & White, M. (2002) Multimedia Augmented Reality Interface for E-learning (MARIE). *World Transactions on Engineering and Technology Education,* 1, 173-176.

Luis-García, R., Alberola-López, C., Aghzout, O. & Ruiz-Alzola, J. (2003) Biometric Identification systems. *Signal Processing,* 83, 2539-2557.

Magalhães, P. S., Revett, K. & Santos, H. D. D. (2006) Critical aspects In authentication graphic keys. *International Conference on Information Warfare and Security (ICIW2006).* Maryland Eastern Shore, USA, Academic Conferences, Inc.

Magalhães, P. S., Santos, H. D. D., Araújo, M. D. D., Fangueiro, R. & Santos, A. C. (2005) Wearable authentication device with biometrical intrusion prevention system. *IADIS* Virtual Multi Conference On Computer Science. Lisbon, Iadis Press.

Schneier, B. (1996) Applied Cryptography: Protocols, Algorithms, And Source Code In C, John Wiley & Sons, Inc.

Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A. & Memon, N. (2005) Authentication using graphical passwords: Basic results. *Human-Computer Interaction International (HCII 2005).* Las Vegas.